

ORIGINAL

DOCKET FILE COPY ORIGINAL

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED

FEB - 7 2000

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of

Communications Assistance for
Law Enforcement Act

)
)
)
)

CC Docket No. 97-213

OPPOSITION OF AT&T CORP.

Stephen C. Garavito
Martha Lewis Marcus
Room 1131M1
295 North Maple Avenue
Basking Ridge, New Jersey 07920

Roseanna DeMaria
AT&T Wireless
Room 1731
32 Avenue of the Americas
New York, New York 10013

February 7, 2000

[Handwritten signature]

SECRETARY

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED
FEB - 7 2000
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)
)
Communications Assistance for) CC Docket No. 97-213
Law Enforcement Act)

OPPOSITION OF AT&T CORP.

AT&T Corp. ("AT&T") hereby submits its opposition to the Petition for Reconsideration filed by the U.S. Department of Justice and the Federal Bureau of Investigation ("FBI") in the above-captioned docket.¹ AT&T opposes the FBI's contentions that the Commission's March 15, 1999 Report and Order ("SSI Order")² must be amended: (1) to permit law enforcement to conduct invasive background investigations on carrier employees, as well as to force employees to execute affidavits of non-disclosure; (2) to mandate a "surveillance status message" capability that the Commission has already determined is not required by the Communications Assistance for Law Enforcement Act ("CALEA");³ (3) to make unnecessary (and overly rigid) modifications to the existing requirement that carriers report security breaches; and, (4) to mandate more onerous recordkeeping requirements.

The FBI's petition, without citation to any additional authority or fact, simply seeks to relitigate issues that the Commission has already carefully considered and rejected. AT&T fully supports the Commission's previous findings and conclusions with regard to these four issues and urges the Commission to reject the FBI's request.

¹ Petition for Reconsideration by the U.S. Department of Justice and Federal Bureau of Investigation, CC Docket No. 97-213 (filed October 25, 1999) ("FBI Petition").

² In the Matter of Communications Assistance for Law Enforcement Act, *Report and Order*, CC Docket No. 97-213, FCC 99-11 (rel. March 15, 1999), *Order on Reconsideration*, CC Docket No. 97-213, FCC 99-184 (rel. August 2, 1999) ("SSI Order").

³ Pub. L. 103-414, 108 Stat. 4279 (1994), *codified at* 47 U.S.C. §§ 1001 *et seq.*

I. PERSONNEL SECURITY OBLIGATIONS

A. The Commission Appropriately Rejected the Proposed Requirement that Carriers Maintain Lists of Designated Employees for the Purpose of Conducting Background Checks.

In its initial comments in this proceeding,⁴ the FBI urged the Commission to require that carriers maintain (and share with law enforcement) a list of all employees designated to conduct electronic surveillance. The proposed list would have included detailed personal information sufficient to allow law enforcement to conduct background investigations of all employees who provision wiretaps. Recognizing the invasiveness of this proposal, the Commission properly rejected it; instead, the Commission required carriers to appoint “senior authorized officer(s) or employee(s)” to provide oversight of electronic surveillance enabled on the carrier’s premises.⁵

The FBI now seeks essentially the same requirements, although claiming that it has narrowed its original proposal by requiring carriers to “include in their lists of designated employees only those employees who, as a regular part of their job duties, are exposed to information identifying the individuals whose communications are being intercepted pursuant to lawful electronic surveillance.”⁶ Nevertheless, the proposed list would still include the employees’ “names, dates of birth, social security numbers, and workplace telephone numbers.”⁷ The FBI would still use this information to conduct background checks on carrier employees involved in ordinary electronic surveillance and “more thorough background checks” on employees who participate in Foreign Intelligence

⁴ Comments of the Federal Bureau of Investigation, CC Docket No. 97-213 (filed December 12, 1997) (“FBI Comments”).

⁵ SSI Order, at ¶¶ 25-26.

⁶ FBI Petition, at 5.

⁷ *Id.*, at 7.

Surveillance Act wiretaps.⁸ The FBI's proposal raises the same privacy and practicality concerns that motivated the Commission to reject the FBI's initial request.

As determined by the Commission in its SSI Order, the collection and dissemination of personal background information about carrier employees is "invasive to carrier personnel and could even compromise a carrier's ability to maintain a secure system by identifying the personnel charged with effectuating surveillance functions."⁹ Section 105 expresses Congress' judgment that law enforcement should not control the actual implementation of wiretaps. On the contrary, telecommunications carriers and their personnel were intentionally placed as a protective buffer between law enforcement and the activation of electronic surveillance. There were several reasons for Congress' decision. First, as discussed in more detail below, the required participation of carrier employees would help protect the "security and integrity" of the carrier's network from unauthorized or unsupervised intrusions by law enforcement personnel.¹⁰ Second, Congress intended the carrier personnel to act as an independent check on law enforcement officials.¹¹ Allowing law enforcement to conduct background investigations of these independent personnel and then to hold that data for long periods without supervision could compromise this check and balance mechanism.

⁸ *Id.*, at 6.

⁹ SSI Order, at ¶ 25.

¹⁰ *See* H. Rep. No. 103-827, at 26 (1994) ("House Report").

¹¹ *See, e.g., id.*, at 17-18 ("Therefore, [CALEA] includes provisions, which FBI Director Freeh supported in his testimony, that add protections to the exercise of the government's current surveillance authority. Specifically, the bill...[r]equires affirmative intervention of common carrier's personnel for switch-based interceptions -- this means law enforcement will not be able to activate interceptions remotely or independently within the switching premises of a telecommunications carrier.").

Moreover, as AT&T pointed out in its original comments, the FBI's proposed rule is unnecessary.¹² Under the Commission's existing regulations, carriers are more than competent to internally monitor security concerns. The certainty of termination from employment and the threat of civil and/or criminal prosecution for the execution of unauthorized surveillance serve as sufficient deterrence against security and privacy breaches. From a privacy standpoint, there is no justification for providing privately-employed individuals' dates of birth or social security numbers to law enforcement. To do so would put the imprimatur of the Commission on law enforcement investigations of these individuals. These are not criminals, targets or suspects -- they are trusted employees of a telecommunications carrier.

Finally, the proposed personnel requirements extend well beyond the scope of CALEA. While CALEA does require carriers to establish policies for the supervision and control of their employees engaged in surveillance, it does not require the identification of, or submission of personal information about, such employees to law enforcement.¹³ Nor does it mandate detailed background investigations of these employees. Thus, AT&T vigorously objects to the FBI's proposal and the invasion of privacy that it represents.

B. The Commission Should Adhere to its Decision Not to Require Execution of Non-Disclosure Agreements.

The FBI has also renewed its request that carriers direct their employees to sign and execute affidavits acknowledging an obligation to protect confidential information about each intercept. AT&T originally commented, and still maintains, that the requirement of a "wiretap affidavit" is

¹² Comments of AT&T Corp., CC Docket No. 97-213, at 32-33 & 36 (filed December 12, 1997) ("AT&T Comments").

¹³ See 47 U.S.C. § 229(b)(1).

among the most intrusive of the proposals offered by the FBI.¹⁴ The proposal appears to assume a lack of professionalism among individuals in the carriers' security departments and suggests a widespread practice of informal discussions about surveillance activities by carrier employees. Nothing could be farther from the truth. As the Commission correctly posits, each carrier will faithfully adhere to "[its] duty to ensure lawfully authorized interceptions of communications or access to call-identifying information" and further administrative precautions are unnecessary.¹⁵

The execution of such affidavits could risk turning matters that would ordinarily be the subject of employee discipline into potential criminal investigations. Today, disagreements between law enforcement and carrier personnel about proper security and privacy measures are resolved by dialogue. Execution of the affidavits could allow the FBI to claim that carrier personnel who deviate from the Bureau's views are subject to criminal investigation for perjury or false statement. But under Congress' scheme, the carrier's personnel are charged with exercising independent judgment about these issues -- even if that judgment occasionally disappoints or angers law enforcement. The independence of these personnel should not be jeopardized by the risk of criminal investigation based on good-faith disagreement with law enforcement about appropriate security and confidentiality measures.

What is more, the proposed non-disclosure agreement is outside the scope of the Act and would merely generate extra administrative burdens in an area in which sufficient protections are already in place. Nowhere does section 105 (or its related provision, section 229) suggest that employees must execute such affidavits. Moreover, as even the FBI admits, "such agreements may replicate

¹⁴ AT&T Comments, at 33.

¹⁵ SSI Order, at ¶ 26.

obligations imposed under existing laws....”¹⁶ The individuals in carrier security departments are professionals and are aware of their existing statutory obligations to preserve the confidentiality of surveillance orders.¹⁷ Since this is the case, there is no reason to impose additional administrative burdens -- ones that are not even required by CALEA -- upon carriers. The Commission should again reject the FBI’s request.

II. SURVEILLANCE STATUS MESSAGE

The FBI again asks the Commission to require that carriers provide a “surveillance status message” capability, which would permit law enforcement to periodically confirm that a wiretap is functioning correctly throughout the carrier’s network. The FBI originally claimed that this feature was mandated by section 103 of CALEA, an argument rejected by the Commission.¹⁸ As demonstrated by AT&T and the vast majority of commentators, such a requirement would have been extremely costly and technically difficult to implement, especially for wireless service providers.¹⁹ The Telecommunications Industry Association concluded that “the FBI’s request is one of the more technically difficult items on their punch list” and noted that the surveillance status message:

would require significant modifications to system architecture to verify electronically that every relevant mobile switch (and every other piece of network equipment containing intercept-related data) is operational and properly configured. No infrastructure is currently in place to permit carriers to poll network equipment in that manner.²⁰

¹⁶ FBI Petition, at 7.

¹⁷ See, e.g., 18 U.S.C. § 2518(8) and 18 U.S.C. § 3123.

¹⁸ In the Matter of Communications Assistance for Law Enforcement Act, *Third Report and Order*, CC Docket No. 97-213, FCC 99-230, ¶ 101 (rel. August 31, 1999) (“Third Report & Order”).

¹⁹ See, e.g., Third Report & Order, at ¶ 99 & n. 187 (citing several comments).

²⁰ Comments of the Telecommunications Industry Association, CC Docket No. 97-213, at 38 (filed December 14, 1998).

As a result, in its Third Report and Order, the Commission properly determined that a surveillance status message is not required by CALEA. Now the FBI takes a second bite at the apple, asserting that the capability is somehow required by a completely unrelated provision -- section 105.

The FBI more or less admits that the Commission was right to reject its original theory based on section 103 (it “does not seek to challenge that ruling”) but asserts that section 105 makes a better home for the requirement of a surveillance status message.²¹ It is difficult to see why this would be the case. The FBI’s filing makes no attempt to explain why the FBI never raised this interpretation of section 105 in any of its nine previous filings in this proceeding (which has lasted more than two full years). In fact, there are two reasons, both fatal to the FBI’s claim. First, the FBI did not adopt this reading of section 105 because it had already asked for this capability under a more plausible part of CALEA -- section 103. Congress made clear that section 103 governs a carrier’s obligation to provide technical capabilities -- like the surveillance status message. The Commission’s rejection of this requirement in the section 103 context thus should have put an end to the FBI’s claim.

Second, the FBI did not adopt this reading of section 105 in its nine previous filings because the reading is contrary to the language and intent of that section. The principal purpose of section 105 was to protect the “security and integrity” of carriers’ systems by ensuring that law enforcement could not activate an interception without a carrier’s permission. Congress’ concern is clearly reflected in the legislative history:

[Section 105] makes clear that government agencies do not have the authority to activate remotely interceptions within the switching premises of a telecommunications carrier. Nor may law enforcement enter onto a telecommunications carrier’s switching office premises to effect an interception without the carrier’s prior knowledge and consent when executing a wiretap under exigent or emergency circumstances under section 2602(c). All executions of

²¹ FBI Petition, at 8.

court orders or authorizations requiring access to the switching facilities will be made through individuals authorized and designated by the telecommunications carrier.²²

Nowhere did Congress suggest that sections 105 and 229 -- which pertain to a carrier's "policies and procedures" -- were also meant to obligate carriers to purchase expensive and complicated technical capabilities to "verify that a wiretap has been established and is still functioning correctly."²³ The Commission properly determined that the surveillance status message was not required by CALEA's technical "assistance capability" requirements (section 103) and it should reject the FBI's belated attempt to mandate the same capability through an unrelated (and inapplicable) statutory provision.

III. REPORTING SUSPECTED COMPROMISE OF SYSTEM SECURITY

Faced with the FBI's original proposal of a two-hour time requirement within which to report breaches of security,²⁴ the Commission appropriately responded to industry concerns and reached a more sensible alternative. Recognizing the difficulties caused by a rigid time limit, the Commission instead required that breaches be reported "within a reasonable period of time upon discovery."²⁵ This outcome takes into account the unknown variables that could possibly cause a carrier to fail a more stringent deadline, like that originally proposed by the FBI.

The FBI now seeks, once again, to impose more restrictive obligations. The FBI's proposal is both unnecessary and overly confining. The SSI Order already requires carriers to "report all acts of unauthorized electronic surveillance."²⁶ The FBI's interpretation of what it thinks is reasonable "in

²² House Report, at 26.

²³ Third Report & Order, at ¶ 97.

²⁴ FBI Comments, at 21.

²⁵ SSI Order, at ¶ 38.

²⁶ *Id.*

light of privacy and safety concerns and the needs of law enforcement” omits a variety of other relevant considerations (such as technical glitches, human error or a carrier’s own internal investigation).²⁷ The Commission reached the appropriate conclusion in establishing a “reasonableness” standard in its regulations and should leave this conclusion unmodified.

IV. RECORDING THE “OPENING OF THE CIRCUIT” FOR LAW ENFORCEMENT

The Commission initially proposed to implement 47 U.S.C. § 229(b)(2) by requiring carriers to record “the start date and time of [an] interception.”²⁸ After carefully reviewing industry and law enforcement comments, however, the Commission modified this directive to require carriers to instead record “the start date and time of the opening of the circuit for law enforcement.”²⁹ Now, however, the FBI seeks to reimpose the very language that the Commission declined to adopt.

The Commission should refuse to modify its language. The Commission has already considered this issue and its recordkeeping regulations reflect practical industry concerns. As the Commission properly realized, carriers routinely maintain, in the ordinary course of business, records necessary to demonstrate good faith compliance with a surveillance order in the event a civil or criminal claim is brought under 18 U.S.C. § 2520.³⁰ For example, in the AT&T Wireless Services (“AWS”) network, the relevant business entity maintains company records of when a circuit is provisioned for law enforcement in response to a lawful authorization. But the method of coordination

²⁷ It also reflects the FBI’s fundamental misunderstanding of section 105, which was intended to protect the carrier’s “*systems* security and integrity” (by preventing law enforcement from activating a wiretap without affirmative carrier intervention) not the “security and integrity of the *electronic surveillance*.” FBI Petition, at 10 (emphasis added).

²⁸ In the Matter of Communications Assistance for Law Enforcement, *Notice of Proposed Rulemaking*, CC Docket No. 97-213, FCC 97-356, ¶ 32 (rel. October 10, 1997).

²⁹ SSI Order, at ¶ 44.

³⁰ *Id.*

between law enforcement and carriers of the actual start time of an interception varies significantly from carrier to carrier and also varies from switch platform to switch platform. In particular, carriers who have several different manufacturers' switch platforms installed within their networks are faced with different protocols for obtaining surveillance start time for each platform. To impose an obligation to reconfigure switches to report the "time at which . . . access to call identifying information was enabled" would require significant technical modifications to AT&T and AWS networks and their vendors' equipment -- another "assistance capability" not required by section 103. The Commission's directive to record the time and date of the "opening of the circuit for law enforcement" is consistent with existing documentary practices and capabilities. The Commission should reject this additional attempt to add yet another section 103 assistance capability that it failed to request in its challenge to J-STD-025.

V. CONCLUSION

The FBI's Petition for Reconsideration adds little or nothing to the pleadings considered and addressed by the Commission in its original decision. For the reasons set forth above, the Commission should again reject the FBI's proposals.

Respectfully submitted,
AT&T CORP.



Stephen C. Garavito
Martha Lewis Marcus
Room 1131M1
295 North Maple Avenue
Basking Ridge, New Jersey 07920

Roseanna DeMaria
AT&T Wireless Services
Room 1731
32 Avenue of the Americas
New York, New York 10013

February 7, 2000

CERTIFICATE OF SERVICE

I, Tracy Rudnicki, do hereby certify that on this 7th day of February, 2000, a copy of the foregoing "Opposition of AT&T Corp." was served by U.S. first-class mail, postage prepaid, to the parties listed below:

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, DC 20535

Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, DC 20530

L. Marie Guillory
Jill Canfield
National Telephone Cooperative Association
4121 Wilson Boulevard, 10th Fl.
Arlington, VA 22203


Tracy Rudnicki

February 7, 2000